AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method of protecting an asset of an information and/or physical type, comprising:

providing processor-based physical asset protection by triggering a user status change upon valid entry or exit through a door of a building;

providing processor-based information asset protection;

integrating said processor-based physical asset protection and said processor-based information asset protection in a centrally-located hosted environment;

making access decisions in accordance with usage patterns of the user by using the integration of the processor based physical asset protection and processor based information asset protection to grant rights to the information systems based on physical access, or independently of physical access, wherein the information asset protection reflects the user status change updated to reflect changes in security access requirements, and wherein usage patterns are calculated by comparing a present usage with historic usage; and

transmitting a breach of physical asset protection in the centrally-located hosted environment such that information asset protection is maintained by denying access thereto.

2. (Previously presented) The method of claim 1, said integrating further comprising:

providing, maintaining and operating a software application that integrates said physical asset protection and said information asset protection in said hosted environment in accordance with user instructions.

3. (Previously presented) The method of claim 1, further comprising:

registering a user by storing user information;

authenticating a user by comparing at least one user characteristic from said user information with a third-party database;

comparing a current asset use pattern with a historical asset use pattern for said user to detect anomalous usage;

updating said historical use pattern on the basis of said current use pattern;

taking a corrective action, wherein a first corrective action is taken if said authenticating generates a non-authenticated user output and a second corrective action is taken if anomalous usage is detected during said comparing; and

wherein said authenticating and comparing provide physical asset protection and information asset protection and are performed in said hosted environment.

4. (Canceled)

5. (Previously presented) The method of claim 1, further comprising:

registering a visitor by providing initial visitor information;

comparing said initial visitor information with a third-party database to determine if said registered visitor is entitled to access to said asset; and

receiving said registered visitor in an authentication area;

checking a match of said registered visitor with a physical entity;

regulating entry on the basis of said checking and comparing, wherein said registered visitor is denied access if said registered visitor does not match said physical entity, or said comparing indicates that said visitor does not have access to said asset; and

wherein at least one of said comparing, said receiving and said checking provide physical asset protection and information asset protection.

6. (Canceled)

7. (Previously presented) The method of claim 5, wherein one of said receiving and said comparing comprises applying biometrics to control access for said user.

8. (Original) The method of claim 7, wherein said biometrics comprises one of scanning and testing a target tissue of said visitor's body.

9. (Original) The method of claim 1, wherein said physical asset protection comprises securing ingress and egress areas for a location protected by a physical barrier.

10. (Canceled)

11. (Canceled)

12. (Currently amended) A system for protecting an asset, comprising:

a physical asset protection module that provides physical protection for said asset by triggering a user status change upon valid entry or exit through a door of a building;

an information asset protection module that provides information security protection for said asset;

an integrator that performs an integration of said physical asset protection module and said information asset protection module, wherein said system is one of in a centrally-located hosted environment and at said asset, the integrator providing integration of the physical protection and information from the information asset protection module for making access decisions in accordance with usage patterns of the user to grant rights to the information systems based on physical access, or independently of physical access, wherein the information asset protection reflects the user status change updated to reflect changes in security access requirements, and wherein usage patterns are calculated by comparing a present usage with historic usage; and

a transmitter for maintaining information asset protection by denying access to the information asset in the centrally-located hosted environment when there is a breach of the physical asset protection.

13. (Previously presented) The asset protection system of claim 12, further comprising:

a user tracking system that authenticates a user as a registered user and provides physical access and information access to said asset in accordance with historical use patterns of said user for said asset, wherein said user tracking system updates said historical use patterns in accordance with a current use pattern of said user.

14. (Original) The asset protection system of claim 13, said historical use patterns comprising at least one of frequency, type and time duration.

15. (Original) The asset protection system of claim 12, further comprising a visitor tracking system that authenticates a registered visitor that has not been barred from accessing said asset, and allows access in accordance with reception authentication process.

16. (Original) The asset protection system of claim 15, further comprising a biometrics authentication subsystem that uses physical data of said visitor to allow said access.

17. (Original) The asset protection system of claim 16, wherein said physical data comprises a test data portion of said visitor's body.

18. (Canceled)

19. (Original) The asset protection system of claim 12, wherein said integration is performed in response to an instruction to develop, maintain and operate a computer application to protect said asset.

20. (Currently amended) A method of providing asset security protection, comprising:

a processor based physical asset protection module transmitting a first signal to a centrally-located hosted environment, said first signal comprising user registration characteristics such that a user status change is triggered upon valid entry or exit through a door of a building;

receiving a second signal from said centrally-located hosted environment indicative of asset access and providing processor based information asset protection; and

using an integration of processor based physical asset protection and processor based information asset protection for making access decisions in accordance with usage patterns of the user to grant rights to the information systems based on physical access, or independently of physical access,

wherein protection of physical and information characteristics of said asset is integrated in said centrally-located hosted environment, [[and]]

wherein the information asset protection reflects the user status change updated to reflect changes in security access requirements, and

wherein usage patterns are calculated by comparing a present usage with historic usage.

21. (Previously presented) The method of claim 20, wherein said transmitting comprises:

providing user registration information to said hosted environment; and

processing at said hosted environment said user information to generate said second signal.

22. (Previously presented) The method of claim 20, wherein said receiving comprises receiving an access decision from said hosted environment, said decision being in accordance with biometrics of a user.

23. (Original) The method of claim 20, further comprising comparing said user information to a third-party database to generate an authentication output as said second signal.

24. (Previously presented) The method of claim 1, further comprising:

entering credentials of a user into an access database in said hosted environment to enroll said user; and

outputting an identification object in accordance with said credentials, wherein unauthorized access is denied by said hosted environment.

25. (Previously presented) The method of claim 23, said entering:

providing an authorized operator with permission to at least one of alter and append said access database;

obtaining a biometric from said user and searching for said biometric in said access database to generate a search result, wherein said biometric and credential data is added to said access database if said search result indicates an absence of said biometric, and if said search result indicates a presence of said biometric in said access database, one of verifying said credential data if said user is authentic and denying access to said user if said user is not authentic, in accordance with said biometric;

denying access to said user if said user appears in a barred user database;

determining if a photo of said user is in said hosted environment, wherein a digital image is imported to generate said photo if said photo is not present in said hosted environment;

verifying that said photo represents said new user;

providing additional user information and user access privileges to said hosted environment; and

generating said identification object having a predetermined layout, said identification object comprising an encrypted three-dimensional barcode in accordance with said biometric and said credential data.

26. (Previously presented) The method of claim 23, said outputting comprising:

receiving said identification object from said hosted environment and producing a copy of said identification object;

said user verifying integrity of said biometric, said photo and said credentials; and distributing said identification object to said user.

27. (Original) The method of claim 25, wherein said identification object is produced by printing an identification badge.

28. (Original) The method of claim 24, wherein said biometric comprises a scan of a biological target tissue.

29. (Original) The method of claim 27, wherein said target tissue comprises at least one of finger, hand and eye parameter.